AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Digital media of Gregory R. Lee seized/recovered from 2659 Sparrow Hill Drive, Columbus, OH, and/or Dublin City Schools and held in FBI Columbus secure evidence storage, 425W. Nationwide Blvd, Columbus, OH 43215

Case No. 2:17-mj-314

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Use of a minor engaged in sexually explicit conduct for purpose of producing a visual depiction of such conduct, in interstate or foreign commerce.
18 U.S.C. 2252	Receipt and/or possession of visual depictions of a minor engaged in sexually explicit conduct, via a means/facility of interstate or foreign commerce

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brett M. Peachey, TFO FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: June 13, 2017

Judge's signature

City and state: Columbus, Ohio

Elizabeth Preston-Deavers, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	
	)	
Digital media belonging to Gregory R. Lee seized and recovered from 2659 Sparrow Hill Drive Columbus, OH and Dublin City Schools and currently held in FBI Columbus secure storage, 425 W. Nationwide Blvd, Columbus, OH 43215	)	**Case No.** 2:17-mj-314

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey ("your affiant"), a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Violent Crimes Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including child pornography offenses and the online exploitation of children.

2. During my career as a police and task force officer, I have participated in various investigations of computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the illegal distribution, transmission, receipt, possession and production of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252.

3. As a task force officer, I am authorized to investigate violations of the laws of the United

States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other subjects and witnesses. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information that would negate probable cause. I have only set forth facts to establish probable cause in support of a search warrant for the following digital media three SanDisk Ultra 3.0 16GB USB thumb drives, one Cruzer Glide 32GB USB thumb drive, one Samsung Galaxy S4 Cell Phone, one Imation 16GB USB thumb drive, one Kingston Data Traveler 256MB USB thumb drive, one Geek Squad 8GB USB thumb drive, one Innovera Technology Essentials 2GB USB thumb drive, one Canon Multi Media Card, one HP Mini 110 Laptop Computer, one Apple Powerbook G4 Laptop Computer, and one Apple MacBook Air laptop computer (hereinafter referred to as "the SUBJECT MEDIA"). The SUBJECT MEDIA, except the Apple MacBook Air laptop, were seized by the Dublin Police Department pursuant to a search warrant executed at 2659 Sparrow Hill Drive, Columbus, OH. The Apple MacBook Air laptop was turned over to Dublin investigators on June 7, 2017, by a representative of Dublin City Schools.

5. The SUBJECT MEDIA to be searched are more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251 and 2252 -the production, distribution, transmission, receipt, or possession of visual depictions of minors engaged in sexually explicit activity.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251 makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce; or if the visual depiction was actually transported or transmitted via any means or facility of interstate or foreign commerce or in or affecting interstate or foreign

commerce.

7. Title 18 United States Code, Section 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct.

8. The term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) as:

A. actual or simulated

i. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

ii. bestiality;

iii. masturbation;

iv. sadistic or masochistic abuse; or

v. lascivious exhibition of the genitals or pubic area of any person.

9. The term "minor" is defined in 18 U.S.C. § 2256(1) as any person under the age of 18 years.

10. The term "visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image, pursuant to 18 U.S.C. § 2256(5);

11. The term "computer" is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

12. The term "child erotica" means "any material, relating to children, that serves a sexual purpose for a given individual." *See* Kenneth V. Lanning, Child Molesters: A Behavioral Analysis (2001) at 65. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child pornography cases. *See United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about pedophiles deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant).

IV. BACKGROUND REGARDING COMPUTERS AND DIGITAL STORAGE DEVICES

13. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of the crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, instrumentalities of crime and/or fruits of crime.

14. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard-drive or other digital/electronic device and can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file on a computer or mobile computing device, the data contained in the files does not actually disappear; rather the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on the hard drive that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

15. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

16. Computers and mobile computing devices (smart phones, tablets, and electronic storage media, hereinafter referred to as "mobile devices" or "mobile computing devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or a mobile computing device with a built in camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such

computerized photographs, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

17. Computers are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera or mobile computing device with video capture capabilities (which is very similar to a regular video camera except that it captures the image in a digital format that can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

18. The capability of computers, mobile devices, and digital storage devices to store images in digital form make them ideal repositories for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB and, in one investigation, your affiant seized a USB drive that could store 128GB of data. The amount of storage space commonly available in home computers and cellular phones has grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

19. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

20. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include KIK messenger service, Snapchat, and Instagram.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

22. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. SEARCH METHODOLOGY TO BE EMPLOYED

23. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment A;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A;

c. surveying various files, directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

VII. INVESTIGATION AND PROBABLE CAUSE`

24. On June 1, 2017, your affiant was advised that the Dublin (OH) Police Department was currently investigating Gregory Lee, residing at 2659 Sparrow Hill Drive, Columbus, OH for engaging in sexual activity with a then fifteen year old female and the production and receipt of child pornography involving the same child. Until recently, Lee was a teacher at Dublin Scioto high school and the victim in this case, hereinafter referred to as Jane Doe, was a student of Lee's.

25. Your affiant obtained reports, narrative supplements, notes and search warrants executed by the Dublin Police Department during the course of their investigation. According to this information, on May 28, 2017, Jane Doe's mother found and read a personal journal belonging to Jane Doe which contained explicit descriptions of at least one act of oral sex between Jane Doe and an individual identified as "Greg Lee."

26. On June 1, 2017, Jane Doe was interviewed at the Child Advocacy Center in Columbus, OH. At that time, Jane Doe advised that she has taken and distributed nude photos of herself to

Greg Lee through both text messages on her phone and through software applications accessed through her phone. Jane Doe also advised that Lee has sent her partially nude photographs of himself which showed his exposed genitalia.

27. In a follow-up interview with Dublin police detectives on June 2, 2017, Jane Doe stated that she had engaged in sexual contact with Lee which started in November of 2016, when she was fifteen years of age. Jane Doe also sent nude photographs or herself, including photos of her masturbating, at Lee's request.

28. On May 31, 2017, a search warrant was obtained by Dublin police detectives for Jane Doe's cell phone and two computers at her residence. During a preliminary forensic examination of Jane Doe's cell phone, a photo of a male's erect penis was recovered. The photo appears to have been sent to Jane Doe through the Viber application. Viber is described as a free, cross-platform instant messaging and voice over IP application which also allows users to exchange images, video and audio media messages by sending files to each other. The date stamp on this photo was May 30, 2017, which correlates to a text conversation found on the phone with a subject utilizing the user name "Bear" through the Viber application. During the interview of Jane Doe at the Child Advocacy Center, Jane Doe advised that Greg Lee's phone number was saved in her cell phone under the name "Bear."

29. On June 2, 2017, Dublin Police Department executed a search warrant at Lee's residence: 2659 Sparrow Hill, Columbus, OH 43219. At that time the SUBJECT MEDIA were seized and transported to the Dublin Police Department. Lee was present at the time and agreed to speak to detectives about the ongoing investigation. Lee admitted that Jane Doe had texted nude photos of herself to him which he then sent to his Gmail account. After being sent to this account, Lee would save the photos to a USB drive which was currently located in his vehicle. The USB drive was also seized from Lee's vehicle, and is included in the SUBJECT MEDIA. Lee also admitted that he utilized an Apple MacBook Air laptop owned by the Dublin City Schools to transfer the files from his Gmail account to the USB drive. Lee had previously possessed the MacBook, but had returned it to the school district several months earlier when he ended his employment there. Lee further added that every photo of Jane Doe that she ever sent to him or that he ever took of her would be on this USB drive. Lee also admitted that he had sent nude photos of himself to Jane Doe but believes that he later deleted them from his devices after sending them to her. Lee further acknowledged that he took photographs of Jane Doe with his phone in his classroom and that these photos would be saved to the USB drive. Both Lee and

Jane Doe admitted that they engaged in oral sex in Lee's classroom at the school multiple times. While Lee did not state that the photos he took of Jane Doe in the classroom were pornographic, based on Lee's tone of voice and body language, as well as the context of the discussion at that time, Dublin PD officers who interviewed Lee believe that the photos Lee took of Jane Doe are likely sexual in nature.

30. On June 7, 2017, TFO Erik Gilleland of the Dublin PD and FBI Child Exploitation Task Force took custody of the SUBJECT MEDIA from the Dublin Police Department property room and transported the items to the FBI Child Exploitation Task Force located at 425 W. Nationwide Blvd. Columbus, OH. The items have thereafter been maintained in a secure storage area pending a search warrant and forensic analysis. That same day, Det. Shull obtained the Apple MacBook Air laptop, which had been in Lee's possession during his employment, from a representative of Dublin City Schools and transported it to the Dublin Police Department where it was secured overnight. The following day, Gilleland transported the Apple MacBook Air laptop computer to the FBI Child Exploitation Task Force where it was stored along with the other SUBJECT MEDIA. The SUBJECT MEDIA was then logged into evidence with the FBI Columbus Resident Agency. To date, no forensic analysis has been performed on any of the SUBJECT MEDIA.

IX. CONCLUSION

31. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2251 and 2252 have been committed, and evidence of those violations is located in the SUBJECT MEDIA described in Attachment B. Your affiant respectively requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 13th day of June 2017.

Elizabeth Preston-Deavers
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A

LIST OF ITEMS TO BE SEIZED

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages) pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
3. In any format and medium, all originals, computer files, copies, and negatives visual depictions of minors engaged in sexually explicit conduct or child erotica.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any visual depictions of minors engaged in sexually explicit conduct.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of visual depictions of minors engaged in sexually explicit conduct.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or sexual acts with minors.
7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show

connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
9. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered..
10. Any and all digital diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED

1) SanDisk Ultra 3.0 16GB USB Thumb Drive
2) SanDisk Ultra 3.0 16GB USB Thumb Drive
3) Cruzer Glide 32GB USB Thumb Drive
4) Samsung Galaxy S4 Cell Phone with Serial Number RV1D55J5Y7Z
5) SanDisk Ultra 3.0 16GB USB Thumb Drive
6) Imation 16GB USB Thumb Drive
7) Kingston Data Traveler 256MB USB Thumb Drive
8) Geek Squad 8GB USB Thumb Drive
9) Innovera Technology Essentials 2GB USB Thumb Drive
10) Canon Multi Media Card
11) HP Mini 110 Laptop Computer with Serial Number CNU9417HG4
12) Apple Powerbook G4 Laptop Computer-No Visible Serial Number
13) Apple MacBook Air Laptop Computer with Serial Number C1MRWMB9H3QD

All of the above items were seized during the execution of a search warrant by the Dublin Police Department at 2659 Sparrow Hill Drive Columbus, OH, or turned over to the Dublin Police Department by representatives of Dublin City Schools and are currently held in FBI Columbus secure evidence storage located at 425 W. Nationwide Blvd, Columbus Ohio, 43215.